IFW

OBLON
SPIVAK
McCLELLAND
MAIER
&
NEUSTADT
P.C.

ATTORNEYS AT LAW

ECKHARD H. KUESTERS
(703) 413-3000
EKUESTERS@OBLON.COM

ZACHARY S. STERN
REGISTERED PATENT AGENT
(703) 413-6509
ZSTERN@OBLON.COM

Docket No.: 217781US2S

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

RE: Application Serial No.: 10/026,813
Applicant: Hiroo NAKANO
Filing Date: December 27, 2001
For: DATA PROCESSING APPARATUS AND MEMORY CARD USING THE SAME
Group Art Unit: 2136
Examiner: HOFFMAN, B. S.

SIR:

Attached hereto for filing are the following papers:

APPEAL BRIEF w/ Reference FIGs. 1-3

Our **credit card payment form** in the amount of **$500.00** is attached covering any required fees. In the event any variance exists between the amount enclosed and the Patent Office charges for filing the above-noted documents, including any fees required under 37 C.F.R 1.136 for any necessary Extension of Time to make the filing of the attached documents timely, please charge or credit the difference to our Deposit Account No. 15-0030. Further, if these papers are not considered timely filed, then a petition is hereby made under 37 C.F.R. 1.136 for the necessary extension of time. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Registration No. 28,870

Zachary S. Stern
Registration No. 54,719

Customer Number
22850
(703) 413-3000 (phone)
(703) 413-2220 (fax)

DOCKET NO: 217781US2S

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF	:
HIROO NAKANO	: EXAMINER: HOFFMAN, BRANDON S.
SERIAL NO: 10/026,813	:
FILED: DECEMBER 27, 2001	: GROUP ART UNIT: 2136
FOR: DATA PROCESSING APPARATUS AND MEMORY CARD USING THE SAME	:

APPEAL BRIEF

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

This is an appeal of the final Official Action mailed November 7, 2005 that presented a final rejection of Claims 1-4 and 11-14, and the Advisory Action mailed April 25, 2006. A Notice of Appeal was timely filed on May 8, 2006.

I. REAL PARTY IN INTEREST UNDER 37 C.F.R. § 41.37(c)(1)(i)

The real party in interest in this appeal is the Assignee KABUSHIKI KAISHA TOSHIBA.

II. RELATED APPEALS AND INTERFERENCES UNDER 37 C.F.R. § 41.37(c)(1)(ii)

Appellant, Appellant's legal representative, and the Assignee are aware of no appeals which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS UNDER 37 C.F.R. § 41.37(c)(1)(iii)

Claims 1-4 and 11-14 are pending in this application. Claims 1-4 and 11-14 have been finally rejected and form the basis for this appeal. Claims 5-10 and 15-20 were previously canceled. The attached claim appendix includes a clean copy of appealed Claims 1-4 and 11-14.

IV. STATUS OF AMENDMENTS UNDER 37 C.F.R. § 41.37(c)(1)(iv)

No amendments were filed after the final rejection, mailed November 7, 2005.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER UNDER 37 C.F.R. § 41.37(c)(1)(v)

The present invention is directed to a data processing apparatus and a memory card, wherein a pseudo data generating circuit is provided so as to generate and output to a data bus pseudo data.

As stated in Claims 1 and 11, the pseudo-data generating circuit generates pseudo-data and outputs the pseudo-data to the data bus in a time interval between a read cycle period and a write cycle period, between a write cycle period and a read cycle period, between two read cycle periods, or between two write cycle periods.

As stated in Claims 3 and 13, the pseudo-data generating circuit is connected to a control signal generating circuit so as to receive a control, and generates and outputs the pseudo-data to the data bus in accordance with the control signal.

For example, Appellant's FIG. 1 is a block diagram of a non-limiting embodiment of a data processing apparatus 10 that includes a CPU 11, a memory 12, an address bus 13, a data bus 14, a read signal line 15, a write signal line 16, a control signal generating circuit 18 and a pseudo-data generating circuit 19, as described in the specification at page 4, lines 4-11. Further, the read control signal and the write control signal to be transmitted to the read signal line 15 and the write signal line 16, respectively may be supplied to the control signal generating circuit 18, and the control signal generating circuit 19 may detect a change in the read control signal and the write control signal and then generate a control signal, as described in the specification at page 5, lines 17-23.

The control signal generated by the control signal generating circuit 18 is supplied to the pseudo-data generating circuit 19, which includes a random number data generating circuit, for example, and which generates pseudo-data including any random number data in accordance with the control signal and outputs the pseudo-data onto the data bus 14, as described in the specification at page 5, line 23, to page 6, line 4.

Further, as shown in the non-limiting example of Appellant's FIG. 2, and as described in the specification at page 7, line 17, to page 9, line 15, the control signal may be supplied to the pseudo-data generating circuit 19 after the read cycle period ends, causing pseudo-data, for example, random number data, to be output onto the data bus 14 after the read cycle period and before the write cycle period.

Note that the following discussion refers to reference FIGs. 1-3, which were attached to the Request for Reconsideration filed April 7, 2006. For convenience, a copy of the reference FIGs. 1-3 is also attached to this Appeal Brief.

In evaluating the claimed invention, it should be understood that the conventional data processing apparatus makes a slight difference in power consumption in accordance with a change in data on a data bus. The change in the data on the data bus is defined as the number of bits changing from 1 to 0 or from 0 to 1. This difference in power consumption is understood by reference to the attached reference FIG. 1 which shows a case where data on the data bus is comprised of 8 bits.

In attached reference FIG. 1, the greater a waveform of the consumed current is, the larger the amount of current will be, and the more data changes, the larger the amount of consumed current. In FIG. 1, "FFH" indicates an intermediate data of a code using a secret key (secret data). When "00H" and "55H" which are before and after "FFH" are fixed data (data read from a memory), a measured consumed current of changed plain text to be input (data to be encrypted) shows the difference of data changing, and the secret key can easily be known.

On the other hand, attached reference FIG. 2 relates to the present invention. In the example shown in attached reference FIG. 2, pseudo-data is output to the data bus in a time interval between two cycle periods such as the read cycle period and the write cycle period so that data changing before and after the cycle periods varies. If the waveform of consumed current is averaged, the data changing will also be averaged. Thus, the data changing cannot be known based on the current consumption.

FIG. 2 shows a case where data on the data bus is comprised of 8 bits. In this example, when data is changed from "00H" to "random number," each bit is either changed from 0 to 1, or is not changed. The probability of data changing in a bit is therefore 1/2, and the average of data changing in an 8-bit data bus will be 8 bits x 1/2 = 4 bits. Then, the all average of data changing will be 4 bits, and thus, data changing cannot be known based on the average consumed current.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL UNDER 37 C.F.R. § 41.37(c)(1)(vi)

Claims 1-4 and 11-14 have been finally rejected under 35 U.S.C § 103(a) as unpatentable over U.S. Patent No. 6,839,849 to Ugon et al. (herein "Ugon") in view of U.S. Patent No. 6,698,662 to Feyt et al. (herein "Feyt").

VII. ARGUMENT UNDER 37 C.F.R. § 41.37(c)(1)(vii)

Applicant respectfully traverses the outstanding rejection because in Applicant's view, the cited references clearly do not obviate the claimed invention.

As explained in the Amendment filed August 12, 2005, Ugon does not disclose a pseudo-data generating circuit which generates and outputs pseudo-data to a data bus. At column 11, lines 14-18, Ugon describes outputs from a random generator (R1), a register (R2), and a timer (R3) that are supplied to a CPU 1 through an interrupt system 15. However, the outputs from the generator (R1), the register (R2) and the timer (R3) are not supplied to a bus (3, 4), as acknowledged at page 3, lines 12-15 of the Official Action mailed November 7, 2005.

In an effort to remedy this deficiency in Ugon, the Official Action mailed November 7, 2005 and the Advisory Action mailed April 25, 2006 rely on column 2, lines 36-42 and column 3, lines 34-52 of Feyt, stating "Feyt et al. (6,698,662) teaches presenting a random data items on the data bus during cryptographic calculation like read and write operations."[1] However, Feyt likewise does not teach outputting the random data items to the data bus. Instead, Feyt indicates that a current consumption I_{out} of an electronic chip 10 is changed in accordance with operations of a central unit 12 or a memory 14 so as to hide an operation of microprocessor card.[2] The random signal generator 28 in FIG. 1 of Feyt does not output random data items to the data bus provided between the central unit 12 and the memory 14. That is, Feyt applies a random current noise to a power supply conductor 22 connected to the central unit 12 and the memory 14[3]. Clearly, the power supply conductor 22 of Feyt is NOT a data bus, and thus this teaching clearly does not remedy the deficiency in Ugon.

Furthermore, while the application of random current noise, as taught by Feyt, may result in an instantaneous variation of the current consumption waveform, if a number of waveforms of consumed current are averaged, the "randomness" in the current waveform introduced by the injected current noise is lost over multiple cycles, such that the random current consumption noise shows a fixed value, as shown in attached reference FIG. 3. In fact, the average waveform of consumed current will show a waveform obtained by adding a certain value to the waveform of attached reference FIG. 1. Therefore, the difference of data changing on the data bus is shown by averaging the waveform, and the secret key may be then be derived. Also, Feyt shows an embodiment of stabilizing the current consumption, and does not show it in detail.

CONCLUSION

Accordingly, as is believed to be evident from the above discussion, the combined teachings of Ugon and Feyt fail to teach generation and application of pseudo-data to a data line, and in fact teach a completely different approach than as claimed. It is respectfully

[1] Office Action mailed November 7, 2005, at page 3, lines 16-19.
[2] Feyt at column 2, lines 36-46.
[3] Feyt at FIG. 1.

submitted that these references clearly do not suggest or obviate the claimed invention and that the claimed invention is patentable over these references.

The rejection applied to Claims 1-4 and 11-14 should therefore be reversed as being clearly improper under the controlling precedent cited above and for the above-noted reasons.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Zachary S. Stern
Registration No. 54,719

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\ZS\21'S\217\217781US\217781 APPEAL BRIEF.DOC

VIII. CLAIMS APPENDIX UNDER 37 C.F.R. § 41.37(c)(1)(viii)

1. A data processing apparatus comprising:

an operation processing unit having at least a read cycle period when said operation processing unit reads data from a device, and a write cycle period when said operation processing unit writes data in the device;

a memory which performs data transmission/ reception between said operation processing unit and said memory;

a data bus connected to said operation processing unit and said memory; and

a pseudo-data generating circuit connected to said data bus, said pseudo-data generating circuit which generates pseudo-data and outputs the pseudo-data to said data bus in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods.

2. The data processing apparatus according to claim 1, wherein said pseudo-data generating circuit generates random number data as the pseudo-data.

3. A data processing apparatus comprising:

an operation processing unit which performs operation processing;

a memory which performs data transmission/ reception between said operation processing unit and said memory;

a data bus connected to said operation processing unit and said memory;

a read signal line and a write signal line connected to said operation processing unit and said memory;

a control signal generating circuit connected to said read signal line and said write signal line, said control signal generating circuit detects a change in a read control signal and a write control signal transmitted to said read signal line and said write signal line, respectively, and then generates a control signal; and

a pseudo-data generating circuit connected to said control signal generating circuit so as to receive the control signal and connected to said data bus, said pseudo-data generating circuit generates pseudo-data and outputs the pseudo-data to said data bus in accordance with the control signal.

4. The data processing apparatus according to claim 3, wherein said pseudo-data generating circuit generates random number data as the pseudo-data.

11. A memory card comprising:

an operation processing unit having at least a read cycle period when said operation processing unit reads data from a device, and a write cycle period when said operation processing unit writes data in the device;

a memory which performs data transmission/reception between said operation processing unit and said memory;

a data bus connected to said operation processing unit and said memory;

an input/output circuit connected to said data bus, said input/output circuit outputs external data onto said data bus and outputs data on said data bus to an external apparatus; and

a pseudo-data generating circuit connected to said data bus, said pseudo-data generating circuit generates pseudo-data and outputs the pseudo-data to said data bus in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods.

12. The memory card according to claim 11, wherein said pseudo-data generating circuit generates random number data as the pseudo-data.

13. A memory card comprising:

an operation processing unit which performs operation processing;

a memory which performs data transmission/ reception between said operation processing unit and said memory;

a data bus connected to said operation processing unit and said memory;

an input/output circuit connected to said data bus, said input/output circuit outputs external data onto said data bus and outputs data on said data bus to an external apparatus;

a read signal line and a write signal line connected to said operation processing unit and said memory;

a control signal generating circuit connected to said read signal line and said write signal line, said control signal generating circuit detects a change in a read control signal and a write control signal transmitted to said read signal line and said write signal line, respectively, and then generates a control signal; and

a pseudo-data generating circuit connected to said control signal generating circuit so as to receive the control signal and connected to said data bus, said pseudo-data generating circuit generates pseudo-data and outputs the pseudo-data to said data bus in accordance with the control signal.

14. The memory card according to claim 13, wherein said pseudo-data generating circuit generates random number data as the pseudo-data.

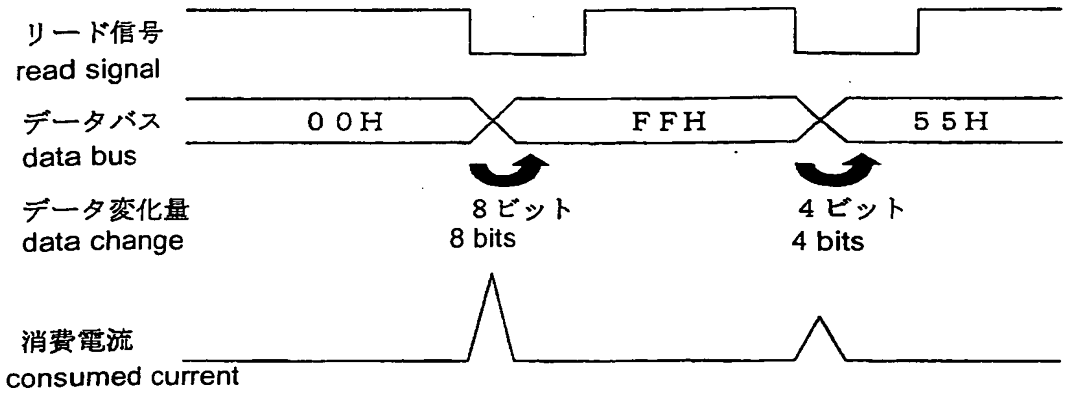
IX. EVIDENCE APPENDIX UNDER 37 C.F.R. § 41.37(c)(1)(ix)

None.

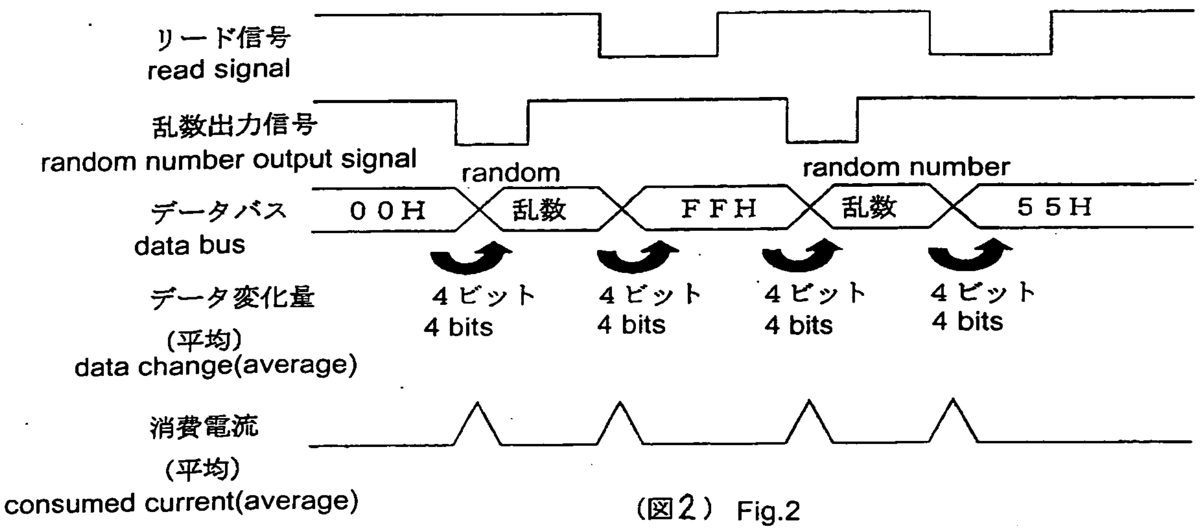
X. RELATED PROCEEDINGS APPENDIX UNDER 37 C.F.R. § 41.37(c)(1)(x)

None.

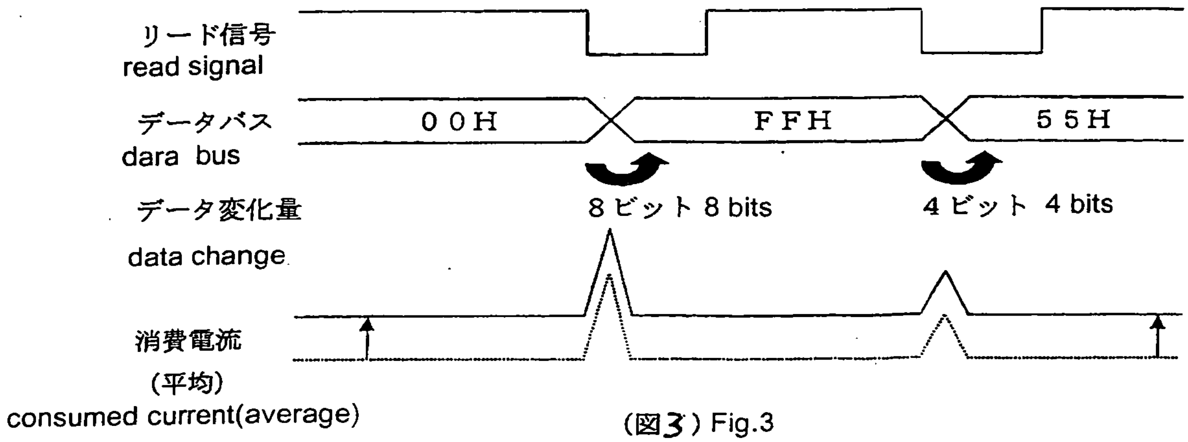
Reference FIGs. 1-3



（図１） Fig.1



（図２） Fig.2



（図３）Fig.3